Cassandra Crossing/ Find My? O Find Me?

(604) — Google comunica perfezionamenti della funzione Find My Device, ormai simile a quella della Mela Morsicata. Ma saranno rose e fiori…

Cassandra Crossing/ Find My? O Find Me?
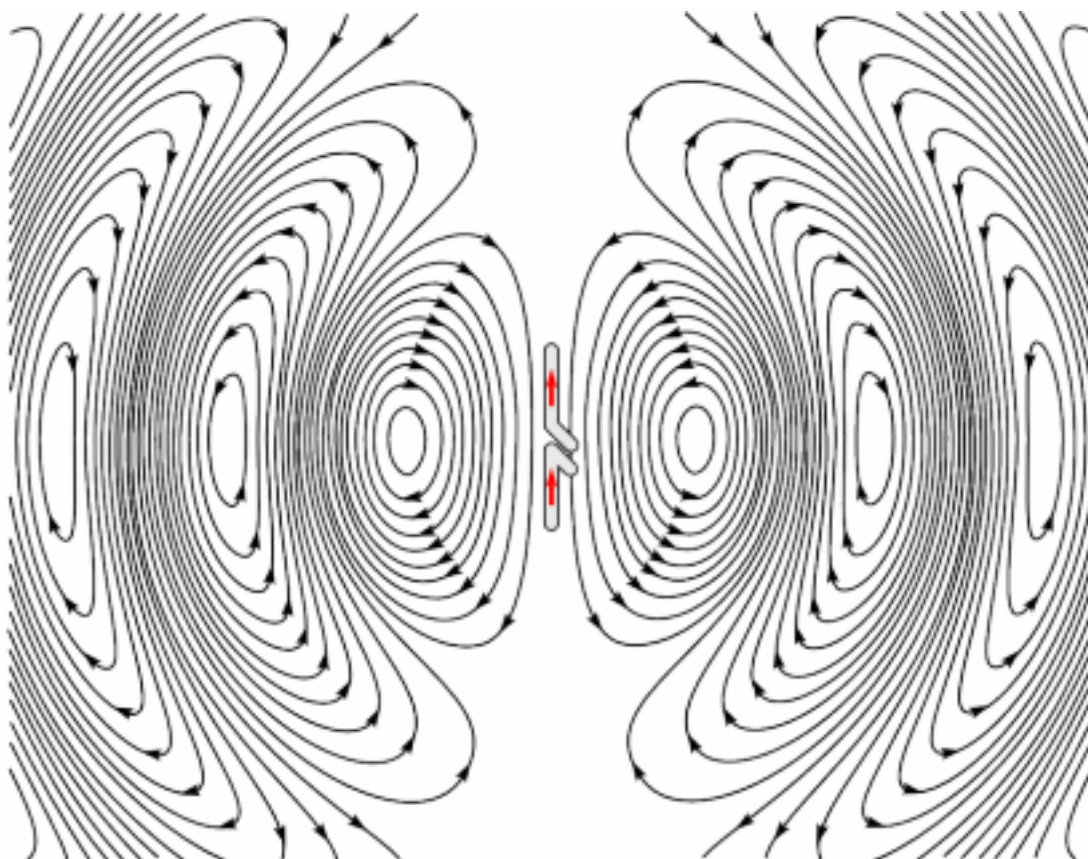
Figure 1: Animazione di dipolo a semionda che irradia (Chetvorno)—CC0

(604)—Google comunica perfezionamenti della funzione Find My Device, ormai simile a quella della Mela Morsicata. Ma saranno rose e fiori oppure no?

1 febbraio 2025—Il covid, ormai meglio mettergli l'iniziale minuscola, ci ha lasciato tanti brutti ricordi, e molti di noi li hanno, consciamente od inconsciamente, in buona parte rimossi. Cassandra però cerca, nei limiti dati dall'età, di ricordarsi sempre quanto più è possibile.

Per cui un annuncio di Google sul miglioramento della funzionalità "*Find My Device*", simile a quella di Apple "*Find My*", ha richiamato alcuni tristi ricordi, proiettandoli nel presente e nel futuro.

"*Ma che ci azzecca il covid?*" penseranno tutti. Ci azzecca, ci azzecca, e ci arriveremo tra poco. Accontenteremo anche i 24 informatissimi lettori, che avranno già pensato "*E' da mo' che in Google c'è questa funzione, che è praticamente uguale a quella di Apple.*" Ma basta giustificazioni; la vostra profetessa preferita è convinta che alla fine i minuti che avrete dedicato a queste righe vi sembreranno ben spesi.

Vediamo quindi il nocciolo della questione, che è espresso in forma generica, e vale quindi per

Android, per iOS e per gli altri sistemi operativi che forniscono, o mai forniranno, funzionalità simili.

Le funzioni di localizzazione dei device richiedono che un utente, titolare di un account di controllo, definisca come "*suoi*" un gruppo di device di qualsiasi tipo, purché dotati di connettività wireless. Da quel momento in poi le informazioni di posizione inviate da ciascun device verranno memorizzate "*nel cloud*" (si vedono le virgolette?) e lì resteranno. Se un device viene smarrito o rubato, il titolare dell'account può interrogare "*il cloud*" e ritrovare le informazioni di posizione del proprio device, in particolare quella attuale, od almeno l'ultima nota.

A seconda del tipo di device smarrito, se questo è ancora online, oltre a tentare di recuperarlo è possibile trasmettergli comandi per far accadere varie cose: emettere un suono, lampeggiare, entrare in modalità "*ascolto*", entrare in modalità "*smarrito*" o "*rubato*", bloccarsi e visualizzare un messaggio sullo schermo, cancellare tutti i dati e tornare alle impostazioni di fabbrica, etc.

Fin qui niente di nuovo. La questione è che, fino a tempi relativamente recenti, la posizione che veniva condivisa era solo quella dei device che "*sapevano dove si trovavano*" (avevano il GPS) e che che il proprietario del device **decideva di condividere**.

Non è una questione da poco. Infatti una opzione di questo tipo, che l'utente può facilmente comprendere, permetteva a chi non fosse contento di seminare i suoi dati di posizione ai quattro venti, di prendere decisioni semplici su cosa e quando far tracciare. Ed inoltre i dati di posizione potevano essere solo quelli forniti dal GPS incorporato, o dalle celle GSM nel caso degli smartphone.

Poi è arrivato Google con la sua idea luminosa. Inventariare e georeferenziare tutte le wifi del mondo, ed usare i nomi (in realtà i MAC) e le posizioni dei router wifi che un device "vedeva" (anche senza connettersi) per localizzare il device stesso. Questo indipendentemente da cosa il possessore del device avesse deciso riguardo al fatto di abilitare o meno la pubblicazione della posizione. Un metodo completamente "passivo", e per Google gratuito, perché "*sottoprodotto*" dei chilometri spesi per fare tutte le foto di Streetview. Il concetto appena enunciato è importante, se vi sembra banale, dovreste rileggere questo paragrafo.

Una parentesi. Vale la pena di ricordare come in Italia il Garante avesse allora chiesto a Google se stesse davvero raccogliendo i dati delle wifi, e Google giurò che non lo facevano apposta, e che i dati raccolti erano stati solo un errore. Quando gli annunci ufficiali successivi hanno rivelato la verità, il Garante è rimasto inattivo. Se ne è dimenticato? O punire chi dice bugie non rientra nelle sue prerogative?

Ma torniamo a noi.

Poi è arrivata Apple, con la sua idea luminosa. Utilizzare anche il protocollo Bluetooth per georeferenziare i device che non possedevano un wifi (tag, auricolari, etc.), e per migliorare la georeferenziazione dei device dotati sia di wifi che di bluetooth.

Curiosamente, la letteratura tecnica in merito non descriveva i dettagli di implementazione, eccedendo invece in assicurazioni di inviolabilità, criptatura ed anonimato dei dati così raccolti. E sia Google che Apple continuano tutt'oggi a rassicurarci che i dati sono criptati, anonimizzati ed "antanizzati". Torneremo dopo su questo punto.

In pratica Apple iniziò a fare la stessa cosa che Google aveva inventato col wifi, utilizzando i device Bluetooth di sua produzione, indipendentemente da chi ne fosse il proprietario, come una rete globale in cui i device bluetooth, facendo "ponte" sui device che erano dotati anche di wifi, fornivano ai server Apple "Find My" la notizia che "vedevano" gli altri device. Non c'era

bisogno di pairing, bastavano i segnali di broadcast, quindi di chi fossero i singoli device non era importante. Bastava ti passassero accanto.

Google si allineò molto rapidamente. Così, attraverso una connessione wifi, ogni device bluetooth fa sapere ad Apple od a Google chi sono gli altri device che vede. E chi conosce la propria posizione e vede un altro device conosce implicitamente anche la posizione dell'altro device più o meno 10 metri, per il solo fatto di vederlo. E la può inviare "a casa". Se poi i due device sono connessi via pairing, può fare calcoli di posizione molto più precisi.

Insomma, si è creata una grande rete omogenea di device che si controllano reciprocamente, e riempiono database "*nel cloud*" di informazioni sulla posizione di tutti i device, e per ovvia (e calcolabile per via informatica) induzione, anche delle persone.

Ed oggi, per mutua convenienza, questo procedimento utilizza device di tutti i produttori.

Ora, non so se questa esposizione vi ha fatto scattare un ricordo; se non fosse successo basta una ulteriore parola; "***Immuni***".

Si, il posizionamento via bluetooth era proprio il modo che Immuni utilizzava per la sua controvesra metodologia di rilevamento del "contatto" con persone positive, e la memorizzazione preventiva e generalizzata di informazioni "anonime" (si vedono le virgolette?) in un cloud era il sistema che ne consentiva il funzionamento.

Non è qui di interesse riparlare di Immuni e della sua maggiore o minore efficacia per l'impiego che avrebbe dovuto avere. Cassandra d'altra parte le aveva dedicato una intera serie di esternazioni, che gli eventuali cultori di informatica retrò (ma neanche tanto) possono trovare qui. Merita forse ricordare come l'opzione che permetteva di disabilitare il tracciamento "anticovid", apparsa tra le opzioni di tutti gli smartphone, sia oggi sparita. L'opzione, non la funzionalità.

E' invece necessario ripetere l'obiezione di fondo contro l'utilizzo di reti globali per la raccolta di dati che localizzino device e persone.

Quando la posta in gioco è stata la sconfitta di una pandemia, era naturale discuterla e tentare di sfruttarla.

Ma ritrovare l'auricolare sinistro che vi è caduto in treno, oppure un device che vi è stato rubato, vale davvero i pericoli che tutti corrono, dovuti alla creazione di una simile banca dati su tutti? Ripeto, su tutti!

Da una parte, anche senza questa rete globale di spionaggio, è tranquillamente possibile localizzare e bloccare un device smarrito o rubato, quando viene acceso.

Dall'altra non è di nessuna rassicurazione il fatto che Apple, Google e gli altri giurino e spieghino che i dati raccolti sono innocui perché anonimizzati. Questo per due ottime ragioni.

La prima è che anche se tutto quello che viene raccontato fosse vero ed esatto, e fosse così dimostrato che le grandi dot.com coinvolte, generosamente e disinteressatamente mantengono una infrastruttura informatica e se ne accollano le spese solo perché non vogliono costringervi ad acquistare un nuovo paio di auricolari (strano, perché ve li venderebbero loro), **questo non impedirebbe che future evoluzioni finanziarie o politiche utilizzassero questi dati e queste infrastrutture per altri e meno nobili fini**.

La seconda è che non si tratta di un problema di buonafede commerciale o di sicurezza informatica. **E' la raccolta di dati "*in sé*" che è pericolosa**, e non dovrebbe essere fatta se non assolutamente necessario, e solo dopo un serio bilancio costi/benefici.

Qualcuno per caso ha appena pensato "*Sembra di sentir parlare del GDPR.*"? Certamente! E' proprio il GDPR, o meglio il tipo di problemi che il GDPR tenta di risolvere.

Sulla questione della raccolta di dati, Cassandra utilizzava nei suoi corsi un paragone; **qualsiasi raccolta di dati deve essere valutata e gestita come un reagente chimico altamente tossico.**

Se il reagente è utile, si considera prima se esistono alternative meno pericolose. Se non ne esistono, si decide di usarlo solo dove serve, nelle minime quantità possibili, per il tempo più breve possibile, smaltendolo poi nella maniera più sicura. Proprio quello che dice il GDPR.

Minimizzazione dei dati raccolti, minimizzazione della estensione della raccolta, minimizzazione del trattamento dei dati, minimizzazione della conservazione dei dati.

Ma è inutile pensare di essere onnipotenti. Non basta scegliere un certo device, consultare letteratura tecnica o leggere blog. Nessuno sa davvero come funzionano queste cose, quando si trovano nella pancia di stati nazione o colossi tecnologici.

E certamente nessuno sa come queste cose potranno malfunzionare, o come funzioneranno, in un prossimo futuro, per quali scopi saranno usate e con quali conseguenze.

Solo un piccolo esempio di cronaca, giusto per ricordare. Pochi mesi orsono alcune femmine umane di alcuni stati di una certa confederazione, che usavano certe app per tener traccia di alcuni propri dati personali, si sono ritrovate ad essere ricercate come criminali, solo per aver esercitato un proprio diritto, improvvisamente diventato un reato. Grazie ai dati gentilmente ceduti.

Come Cassandra ama ricordare, **l'unica possibilità che è rimasta per gli individui** che devono vivere nella realtà tecnologica che ci circonda, **è quella della riduzione del danno**. Ogni nuova applicazione o servizio deve essere usato con criterio, e solo se serve. Il fascino della novità, in questo caso, è un nemico contro cui lottare.

Quindi è indispensabile fare la fatica di decidere se adottare alcuni comportamenti, come spegnere il bluetooth dove e quando possibile, oppure non registrare i propri device sui propri account personali, o su servizi tipo "*Find My*", a meno che non sia utile o necessario. E farlo invece tranquillamente, ma solo se e quando davvero serve, e solo se non si vedono controindicazioni.

Oppure lasciarsi trascinare dalla corrente delle mode, far finta che il tecnocontrollo sociale sia un'invenzione di paranoici di professione come Orwell o Cassandra, e diventare Eloi *tecnologicamente generati.*

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on February 2, 2025.

Canonical link

Exported from Medium on August 27, 2025.